Secure Deployment and Disposal

Bezbedna implementacija i otpisivanje sistema

Implementacija informacionog sistema ili postavljanje sistema u produkciju je složen proces uvođenja informacionog sistema u radno okruženje i omogućavanje njegove upotrebe od strane korisnika koji se sastoji iz više faza:

- **Priprema okruženja za sistem** (instaliranje i konfigurisanje hardvera, softvera i mrežne infrastrukture neophodne za rad sistema, postavljanje servera, baza podataka, mrežnih rutera i drugih komponenti)
- **Instalacija informacionog sistema** (prenos aplikacija, konfiguracija sistema, podešavanje parametara i integraciju sa drugim sistemima)
- **Testiranje sistema u produkciji** (funkcionalnosti sistema, performansi, bezbednosti i integriteta podataka)
- **Puštanje sistema u radno okruženje** (omogućavanje pristupa korisnicima i početak stvarne upotrebe sistema za obavljanje poslovnih ili operativnih aktivnosti, obučavanje korisnika za pravilno korišćenje sistema)
- **Podrška i održavanje** (rešavanje eventualnih problema koji se mogu pojaviti, ažuriranje sistema kako bismo održali stabilnost, sigurnost i funkcionalnost)

Bezbednost je kritična tačka svakog sistema, te ona (tj. njen nedostatak) predstavlja jedan od najvećih problema pri implementaciji novog sistema. Kako bismo osigurali sigurnost sistema, pri izvršavanju svake faze implementacije moramo preduzeti mere predostrožnosti.

Prvi korak za uvođenje ovih mera zapravo počinje mnogo pre implementacije, čak i pre same izrade sistema. Identifikacija sigurnosnih zahteva se vrši tokom dizajniranja sistema. Ona uključuje identifikaciju potencijalnih pretnji, ranjivosti i opisivanje ostalih sigurnosnih funkcionalnosti. Na osnovu identifikacije se izrađuje politika bezbednosti. U njoj se jasno definišu smernice, pravila i procedure koje se odnose na bezbednost sistema. Na našem projektu, politika bezbednosti bila je definisana specifikacijom.

Tokom izrade sistema potrebno je implementirati politiku bezbednosti, koja na našem projektu uključuje:

- zaštitu mrežnog saobraćaja (putem HTTPS-a),
- višefaktorsku autentifikaciju,
- restrikcije pristupa,
- upravljanje privilegijama i
- nadzor pomoću logova i alarma.

Ove mere obezbeđenja spadaju u utvrđivanje sistema (system hardening), tehnički deo implementacije politike bezbednosti. Utvrđivanje sistema uključuje i redovno ažuriranje i *patching* sistema, kao i zaključavanje sistema. Zaključavanje podrazumeva onemogućavanje pristupa ili brisanje nepotrebnih servisa i funkcionalnost, kako bismo smanjili moguće ulaze u sistem koje potencijalni napadači mogu da iskoriste.

Priprema za implementaciju sistema

Tokom pripreme okruženja za sistem potrebno je obezbediti infrastrukturu na koju softver leže. Ovo obuhvata sigurnost harvera, ali i operativnog sistema servera.

Za osiguranje harvera najbitnija je fizička bezbednost. Fizički pristup serverima je najlakši način za kompromitovanje servera, pa je kontrolisanje pristupa i ulaza (ključevi, ključ-kartice, biometrijska identifikacija) u serverske sale ključni deo zaštite hardvera.

Onemogućavanje nekorišćenih portova na mrežnoj opremi može smanjiti moguću površinu napada na hardverskom nivou, a održavanje redovne inventure hardvera može otkriti neovlašćeno dodavanje ili uklanjanje komponenti. Pored toga, redovno održavanje i ažuriranje *firmware*-a smanjuje šansu sigurnosnih propusta i dopuštanja ranjivosti.

Prilikom konfigurisanja hardvera i operativnih sistema, bitno je ograničiti pristup samo autorizovanim korisnicima i konfigurisati jaču autentifikaciju za pristup administrativnim funkcijama. Kako su lozinke najčešća vrsta autentifikacije u informacionim sistemima, potrebno je koristiti jake lozinke za sve administratorske naloge i redovno ih menjati.

Korisnicima treba davati samo neophodne privilegije; svaki korisnik treba da ima pristup minimalnom skupu funkcionalnosti. Važno Potrebno je i konfigurisati *firewall* kao i *IDS/IPS* sisteme kako bismo kontrolisali pristup sistemu i detektovali potencijalne napade. Dobra praksa nalaže i generisanje logova koji beleže svu aktivnost na sistemu kao i redovno pravljenje rezervnih kopija.

Postavljanje sistema u produkciju

Nakon izvršene pripreme, radi se *staging. Staging* okruženje treba da bude blisko produkcijskom okruženju. U ovom okruženju se vrši testiranje sistema, među kojima je za proveru sigurnosti sistema specifično *penetration* ili pen testiranje.

Ako testiranje prođe uspešno, prelazi se na migraciju podataka i integraciju sistema. Migrirane podatke treba validirati i potvrditi da je održan njihov integritet i doslednost. Kada su svi podaci uspešno dovedeni u *staging* okruženje, vreme je da se napiše sistemska dokumentacija i trening materijali za korisnike. Korisnike onda treba podučiti korišćenju sistema.

Kada su korisnici obučeni, prelazi se sa *staging* okruženja na produkcijsko. Treba osigurati da je ono spremno za rad i da ispunjava zahteve za hostovanje sistema. U ovo spada potvrđivanje uređenja infrastrukture, bezbednosnih mera i eventualne integracije sa drugim sistemima. Potrebno je na isti način migrirati i validirati podatke kao i u prethodnoj fazi.

Kada su svi podaci preneti potrebno je namestiti autorizaciju i pristup - korisničke naloge i uloge, kao i mehanizme autentifikacije. Potom se rade *pre-go-live* provere, korisnicima se pružaju potrebne informacije i odgovori na eventualna pitanja. Kada su sva pitanja zbrinuta izvršava se *go-live* plan i tranzicija na produkcijsko okruženje.

Nakon samog *deployment*-a ostaje pružanje podrške i održavanje softvera. Ovo uključuje ispravljanje grešaka, ažuriranje i tehničku/korisničku podršku. Proces pružanja podrške traje sve dok je sistem u funkciji.

Otpisivanje sistema

Prestanak rada sistema podrazumeva trajno uklanjanje informacionog sistema, hardverske opreme, podataka i ostalih resursa koji se više ne koriste. Bezbedno otpisivanje sistema je neophodno kako bi se osiguralo pravilno uništenje osetljivih podataka i sprečilo njihovo ponovno korišćenje.

Kako bi se uništenje izvršilo, prvo je potrebno identifikovti sve osetljive podatke (lični, finansijski, zdravstveni i sl.). Nakon toga, oni se brišu iz sistema; da bi bili obrisani na bezbedan način, potrebno je pri brisanju koristiti specijalizovane alate ili procese za trajno brisanje (*wipe*) podataka iz baza, sa diska ili drugih medija.

Ovaj postupak treba da osigura da se podaci ne mogu obnoviti ili povratiti nakon otpisivanja sistema. Nekada je radi uništavanja podataka potrebno uništitin i hardversku opremu za skladištenje podataka kao što su hard-diskovi ili *solid state* diskovi. Nakon uništenja podataka, potrebno je izvršiti i verifikaciju uništenja.

Prilikom otpisivanja sistema, važno je pravilno dokumentovati sve korake koji su preduzeti. Ovo uključuje beleženje datuma otpisivanja, vrste podataka koji su uništeni, metode koje su korišćene za brisanje ili uništavanje podataka i druge relevantne informacije. Ova dokumentacija služi kao svedočenje o bezbednom otpisivanju sistema i može biti neophodna u slučaju revizija, pravnih ili regulatornih zahteva.

U vezi sa tim, tokom celog postupka neophodno je poštovati važeće zakone, propise i regulative u vezi sa zaštitom podataka i bezbednošću informacija. Ovo može uključivati usklađenost sa GDPR-om (Opšta uredba o zaštiti podataka) ili drugim lokalnim zakonima i propisima.